MEDICAL IMAGE SECURITY USING ENHANCED HONEY ENCRYPTION AND OPTIMIZATION TECHNIQUES

A SYNOPSIS

Submitted by

JAYAHARI PRABHU G

(Reg. No. 201808160)

in partial fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRONICS ELECTRICAL AND BIOMEDICAL TECHNOLOGY

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL-626126

TAMILNADU, INDIA.

SEPTEMBER 2022

1. INTRODUCTION

With the improvement of medical imaging techniques, security is a basic requirement for all applications to protect the stored data and transmit it over a network, as given by Avudaiyappan et al. [1]. The Internet will trade in medical imaging techniques and digital image applications with extensive changes in connectivity and technology. Digital images play a nominal role in today's communication. Whereas the encryption technique for security is a process to convert data into an unreadable format by unauthorised users using cryptographic algorithms to preserve data. The better algorithms will meet the requirements of security, protecting the encryption components. The best part of simple encryption calculations is used as content details or matched data, shown by Shankar et al. [2].

This information on cryptographic algorithms can be used to provide various security methods, such as privacy, validation, uprightness, and authorization. There are standard cyphers such as AES, DES, and RSA that cannot be used for medical image security optimization Shankar et al. [3]. The widely used optimization algorithms like Grasshopper Optimization (GO), Blowfish Optimization, and Signcryption Optimization have the disadvantage of using primary ciphers, which require higher system power and computational time. The hybridization of HE with BPSO is performed to attain the optimization of keys, using the primary parameter "PSNR", given by Elsohney et al. [4]. It is important to ensure the value of encryption for medical information, shown by Guhan et al. [5]. The proposed work is on hybridising the HE algorithm with BPSO for medical security. It is used to keep sensitive data more secure, and it will be tedious for unauthorised users to access. This cryptographically based protection helps to provide the required security data or information by using a symmetric and asymmetric key encryption scheme to classify a restorative medical image to any unintelligible configuration.

Some existing algorithms do not handle all optimization issues, even though most of them could take care of a variety of problems, shown by Shankar and Lakshmanaprabhu [6]. Here we proposed hybridising the HE algorithm with the BPSO technique. The data about efficient image encryption security is supplied with authentication. The proposed work focuses on hybridising an encryption technique that could easily handle certain issues, with an optimization technique given by Shehab et

al. [7]. Section II explains the literature review, Section III explains the objectives, and then the research problem is identified and the result of the proposed work is explained in Section VII. This proposed work is concluded with Performance analysis.

2. LITERATURE REVIEW

In 2018, Hua et al. [8] proposed a new encryption method for storing medical files. It has high productivity and shows the power to safeguard some loss of impulse data. Initially, some irregular data is embedded in the image's environmental variables. It is possible to easily apply the proposed encryption plan to medical images with any design mentioned. It gives two kinds of flexible dissemination tasks to execute the pixel: bitwise XOR and modulo arithmetic numbers. Reproduction and evaluation plans possess a high degree of security due to their bitwise XOR and modulo arithmetic number functionality. These plans work rapidly and could more readily conform to interference with impulse noise and data loss. Praveenkumar et al. [9] in 2018, proposed an increased need for effective data processing of medical images in telemedicine applications. Even though a protected set is apportioned to each device, the users concerned leave it unused more often than not. Cognitive Radio (CR) is an invention that uses the new spectrum range by adopting the principle of range detection. This paper proposes an efficient and safe transmission of medical images by embracing CR innovation and image encryption protocols. Initially, to scramble the image successfully, the latest encryption is suggested. The range detection strategy is done via Universal Software Radio Peripheral (USRP) to detect the new recurrence band to communicate the encoded bio-signal. The proposed encryption calculation consolidates the grouping operation of DNA (Deoxyribose Nucleic Acid) and clamorous guides to encode the DICOM image pixels effectively. Test results are obtained through different investigations. El-Latif et al. [10] provided a novel methodology for efficiently encrypting medical data in a quantum encryption manner. Chaotic and gray codes are used in the proposed calculation. The composite quantum image is encoded at that stage using a quantum XOR activity based on a key generator restricted by the logistic-sine map. Based on the NEQR quantum picture portrayal, the circuits of the proposed encryption/unscrambling calculation are planned. Research in mathematics and simulation shows that the method of quantum image encryption proposed is highly efficient and feasible. Thakur et al. [11] proposed utilising a controlled-NOT gate to

show the added data's security in 2018. Initially, the hidden quantum image must be jumbled. The encoded concealed image is put into the quantum cover image by using the two most and least important qubits. The quantum watermark image, mixed using the Arnold cat map, is then implanted using the two least and major qubits into the quantum transporter image. The novelty of the proposed work has been represented by various approaches with outstanding visual quality and a high level of implantation and safety. In 2020, Gupta et al. [12] proposed a watermarking-based approach for medical image security, which is proposed in this paper. Here, non-sub-sampled contour let change (NSCT), singular value decomposition (SVD), and redundant discrete wavelet transform (RDWT), which are used for improving strength and capability by applying 2-D in the security system. In this system, the medical image is applied to get higher entropy. RDWT will be then applied to the NSCT input image, while the RDWT coefficient of the isolated vector is calculated. A comparative technique is used for both Watermark medical images. The encryption here makes the methodology safe and secure for medical applications. Saddam et al. [13] presented a lightweight security scheme based on the session key in this paper, which was published in 2020. In this study, a new session key is generated with each image encryption, with genetic algorithm crossovers and session keys regulated by mutation. The Lightweight cryptography technique employs 64-bit plain text. Zeng et al. [14] It has an 80-bit key for encrypting the picture and 64-bit key crossover and mutation operators. The lightweight algorithm performs well for all colour and grayscale photos. Under the MATLAB 2017 environment, the proposed approach is simulated, and various parameters are compared to similar kinds of the existing scheme. More contemporary works have been discussed regarding Grasshopper Optimization, which facilitates the presumptions required and creates an optimization generation schedule due to group interactions, and the Multi-Verse Optimizer defined by Mirjalili et al. [15] that explained the functionality of White, Black, and Wormholes in the dataset using adaptive WEP and TDR values. They fall in comparison with the key update and password maintenance mechanisms.

We proposed combining the HE Algorithm with the ALO method in this paper by El-Latif et al. [16]. Authentication is provided with the information on the effective image encryption security. The proposed research aims to combine an encryption technology that can readily address the key updation a trap construction mechanism

with an optimization method. The review of literature is explained in Section II. The proposed method is detailed in Section III, preceded by the model's outputs, which are described in Section IV.

3. OBJECTIVES OF THE WORK

The main objectives of this research work are

1. To develop a novel image security algorithm using honeypot encryption techniques with Ant-Lion optimization and evaluate it with standard performance measures.
2. To develop a modified honey algorithm for better performance.
3. Implementing Modified Honeypot Encryption for Securing the Medical Imaging Data
4. Multimodal Medical Imaging Security Using Hybridization of the Honey Encryption Algorithm with Binary Particle Swarm Optimization.

4. RESEARCH PROBLEM

Every network that sends and receives data needs to be secure in some way. Medical imaging technology is one of the most critical applications that necessitates data protection. Particularly if you need to keep track of any important patient information. This medical imaging system employs encryption and decryption. Ismail et al. [17] Using a number of cryptographic techniques, the security key was established to protect the data. Choosing an algorithm for secure data transfer in order to accomplish quality aspects like greater privacy, secrecy, integrity, and efficiency. The proposed study uses a variety of ways to hide vital health information, including the Honey Encryption Algorithm and the Antlion optimization methodology. In Ma et al. [18], comparison to the preceding one, honey yields a better result. Throughout encryption and decryption, the Ant Lion optimizer uses random keys. After that, the updated key is optimised by analysing every element and generating paths that trigger the traps and latching functions.

5. CONTRIBUTIONS

The Honey Algorithm Encryption is compared to current methods such as GO-PSO, the Signcryption Method, and Blowfish using OFP assessment measures. The medical imaging is then encoded using known techniques, as well as a relative investigation of entropy and key sensitivity. HE algorithm transmits the safe and reliable way of medical image. Furthermore, decoding is completed at the end to assess information comprehension. The proposed technique has a low mean square error because it seems distinctive from the other equivalent algorithm. Standard processes are then used to encrypt the medical images, including a comparison of entropy and key sensitivity. The HE algorithm is a secure and reliable method of transmitting medical images. Decoding is also conducted in the end to confirm that the material is comprehended. The comparison of the entropy system for GO-PSO, the encryption approach, blowfish with OFP, and the proposed algorithm is shown. It has a low error rate and is put through its tests with a number of image security assessments.

6. ORGANIZATION OF THE THESIS

The research work is organized into four chapters and is as follows:

Chapter 1

This chapter covers the Honey Encryption Algorithm, which is optimised with the Ant-Lion optimizer. HE is used to extend the safety of medical imaging techniques. In Ant-Lion optimization, both the private key and the public key are optimised during the encryption process.

Chapter 2

This chapter covers the blowfish algorithm and the honey algorithm, which are used to extend the safety of medical imaging techniques. Here it is used to optimise the cryptographic keys during the encryption process. Performances of the honeycomb encryption technique that are raised and evaluated by using PSNR, MSE, CC, and Entropy are better than those of the blowfish algorithm. The entropy maximises with the Honeycomb encryption model, and the PSNR value seems to be higher than the blowfish algorithm.

Chapter 3

This chapter covers ALO along with the encryption algorithm Honey is used to enhance the security of medical imaging technologies. As compared to other existing algorithms for specific parameters, the HE technique properly estimated PSNR and MSE. Honey is superior to the previous one in terms of results. The Ant Lion optimizer uses random keys for encryption and decryption.

Chapter 4

This chapter covers the HE algorithm, which is optimised to extend the protection of medical imaging techniques with BPSO cryptographic keys that have been optimised by 1% using the Honey Algorithm during the encryption process. Compared to the same parameters with other existing algorithms, the HE algorithm efficiently estimated PSNR and MSE. The SSI maximises in the HE algorithm, and the PSNR value seems to be higher than the other existing algorithms. This honeycomb algorithm reduced computation time. Hence, the efficient image encryption security is discussed using Honey Algorithm with optimization Technique.

7. OVERVIEW OF SEGMENTED RESULTS

The encrypted and decrypted images along with their performances for various images have been demonstrated in Figure 1 for the proposed HE-ALO technique.

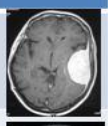
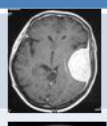
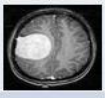
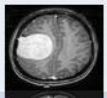
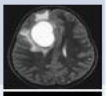
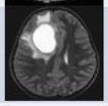
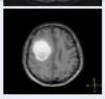
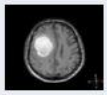
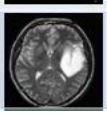
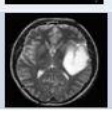
Images	Encrypted Images	Decrypted Images	PSNR	MSE	CC	ENTROPY
			59.61	0.019	1	7.80
			58.90	0.013	0.99	8.02
			56.22	0.02	0.97	7.91
			57.86	0.031	0.96	7.85
			57.78	0.06	1	8.02

Figure 1. Medical Imaging Data Security using Effective Honey with Ant-Lion optimization.

The MSE values demonstrated for the above dataset has been evaluated with Honey encryption algorithm and compared with that of Blowfish algorithm, as shown in Figure 2.

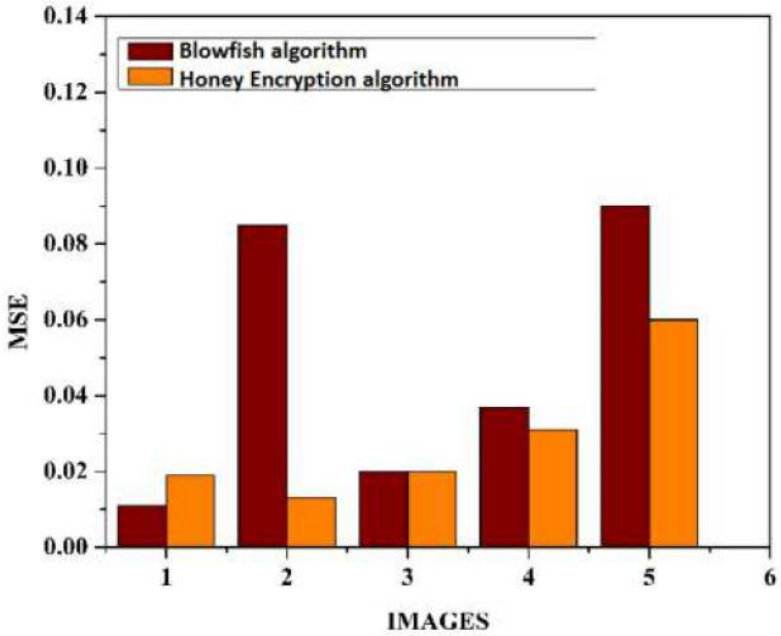


Figure 2. Image Security Performance for MSE.

The PSNR values demonstrated for the above dataset has been evaluated with Honey encryption algorithm and compared with that of Blowfish algorithm, as shown in Figure 3.

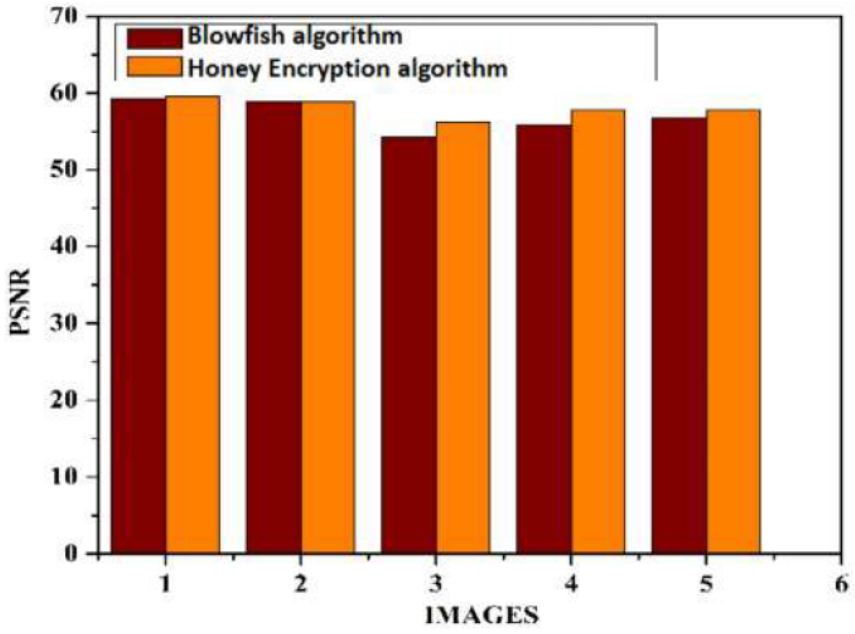


Figure 3. Image Security Performance for PSNR.

As shown in Figure 4, the Entropy values for the dataset mentioned above have been assessed using the Honey encryption technique and contrasted with those of the Blowfish algorithm.

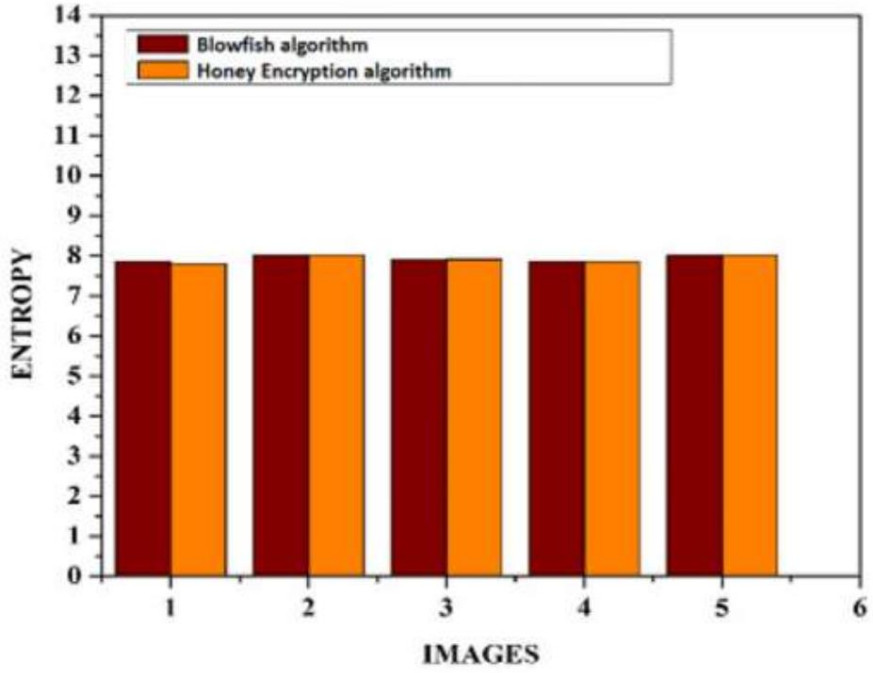


Figure 4. Image Security Performance for Entropy.

The CC values for the dataset mentioned above were assessed using the Honey encryption technique and contrasted with those of the Blowfish algorithm, as shown in Figure 5.

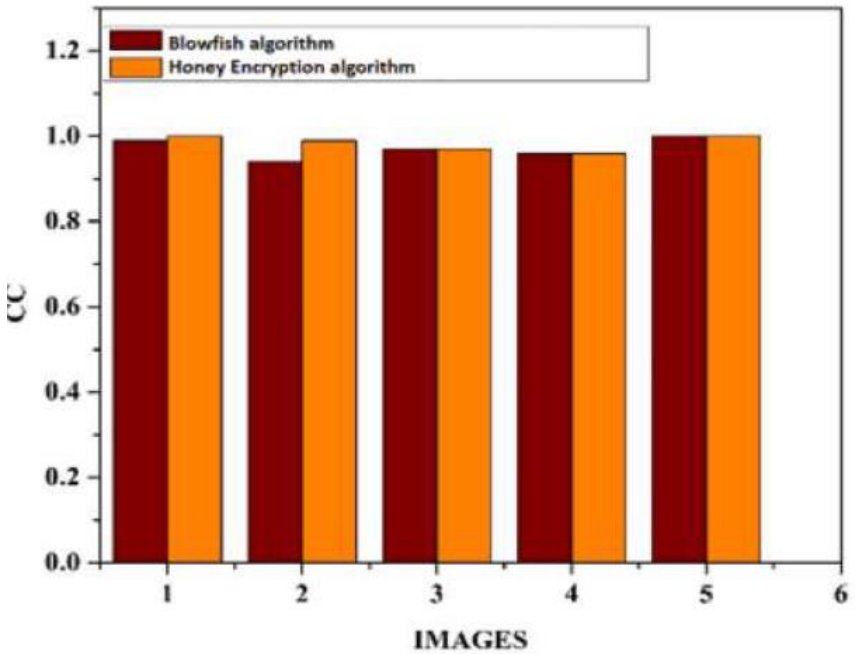


Figure 5. Image Security Performance for CC, using Honey encryption algorithm.

The encryption technique using HE and ALO hybridized technique for 12 different medical image sample has been demonstrated in Table 1.

Table 1: Variation in decryption and encryption images in terms of PSNR for Brain web dataset.

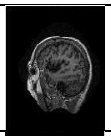
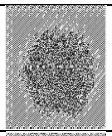
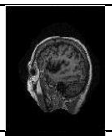
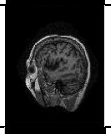
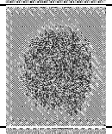
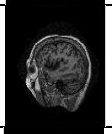
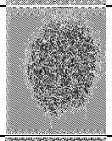
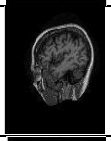
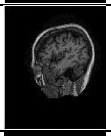
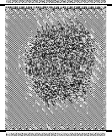
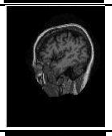
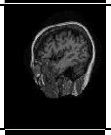
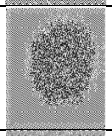
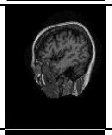
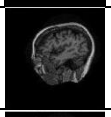
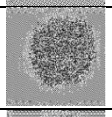
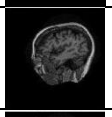
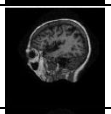
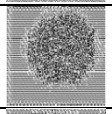
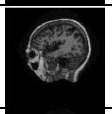
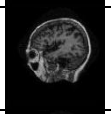
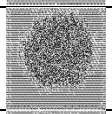
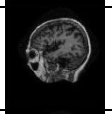
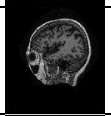
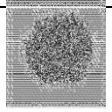
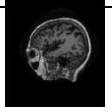
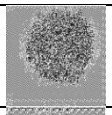
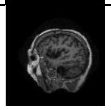
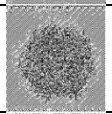
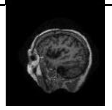
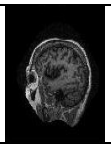
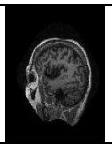
Input	Images	Encrypted Images	Decrypted Images
Input1			
Input2			
Input3			
Input4			
Input5			
Input6			
Input7			
Input8			
Input9			
Input10			
Input11			
Input12			

Table 2 shows the PSNR performances of different medical images evaluated using the proposed HE-ALO approach compared with other conventional algorithms.

Table 2: An Efficient Image Encryption (HE) approach Comparative Result in terms of PSNR for Brain Web dataset

GO-PSO	**Signcryption Algorithm**	**Blowfish with OFP**	**Honey Encryption Algorithm with Ant-lion optimization (Proposed)**
Peak Signal Noise Ratio (PSNR)			
59.51	59.54	59.61	59.69
58.70	58.76	58.90	59.93
55.22	55.76	56.22	57.21
55.86	56.86	57.86	58.89
54.73	56.78	57.78	58.79
57.31	57.39	59.31	59.91
56.32	56.79	57.32	58.31
57.32	57.48	58.32	58.39
56.90	57.90	58.90	58.94
57.80	57.89	57.83	58.89
57.62	57.69	59.62	59.69
56.71	57.76	57.79	59.79

The average prediction of the HE algorithm is greater than the other current algorithms, according to a comparative study made. The MSE estimates the error and offered values by the various soft computing techniques revealed in Table 3.

Table 3: An efficient Image encryption (HE) approach comparative result in terms of PSNR for Brain web dataset.

GO-PSO	**Signcryption Algorithm**	**Blowfish with OFP**	**Honey Encryption Algorithm with Ant-lion optimization**
Mean Square Error (MSE)			
0.11	0.019	0.019	0.011
0.13	0.013	0.013	0.011

0.14	0.02	0.02	0.02
0.19	0.10	0.031	0.019
0.013	0.08	0.06	0.04
0.11	0.05	0.05	0.02
0.11	0.07	0.08	0.02
0.19	0.11	0.02	0.02
0.14	0.11	0.11	0.07
0.13	0.09	0.02	0.02
0.11	0.07	0.05	0.04
0.19	0.11	0.08	0.04

The peak signal to noise ratio of several protective computations is demonstrated by the proposed hybrid technique. In the defined approach, the peak signal to noise estimation. Honey encryption is nearly identical and does not change substantially. Figure 6 shows the PSNR observation of the performance of the given approach to other conventional methods.

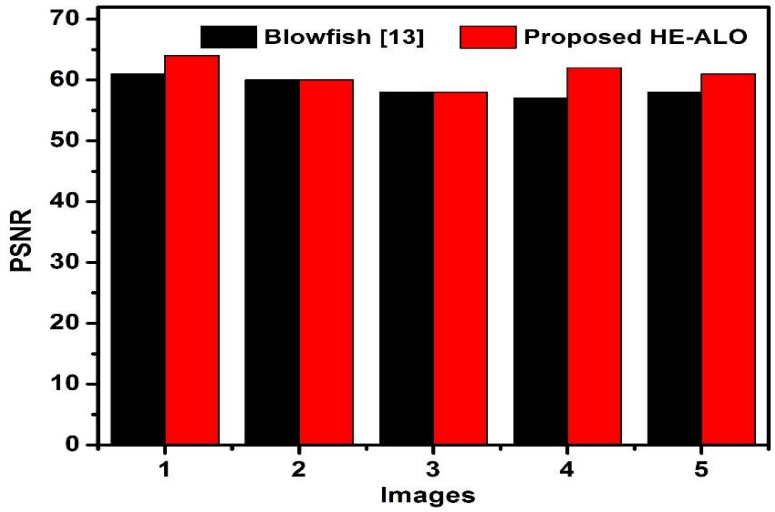


Figure 6. Comparison of PSNR values for the proposed HEALO with Blowfish algorithm from literature.

Figure 7 displays a comparison of the Mean Square Error for the proposed hybrid approach compared along with the Blowfish.

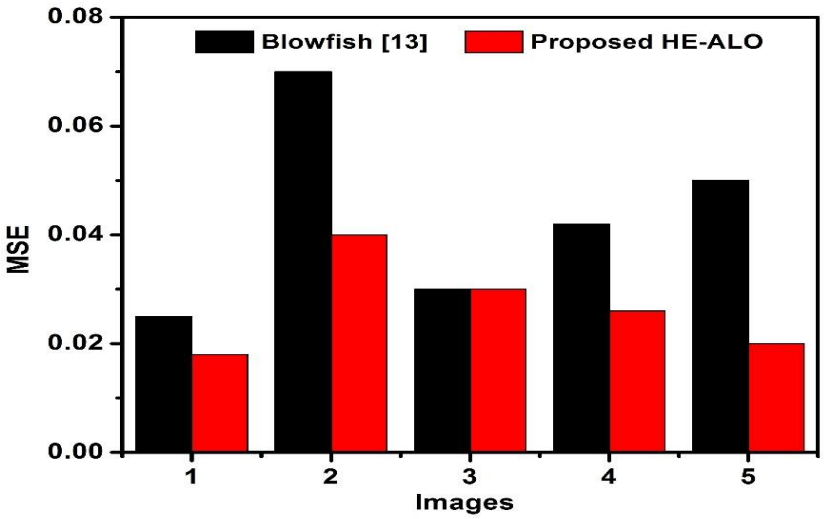


Figure 7. A comparison of the MSE values for the proposed hybrid HE-ALO technique compared with the Blowfish algorithm.

The Correlation coefficient of the proposed technique proves superior compared to the existing blowfish algorithm as depicted in Figure 8. When an analysis is performed for 5 images.

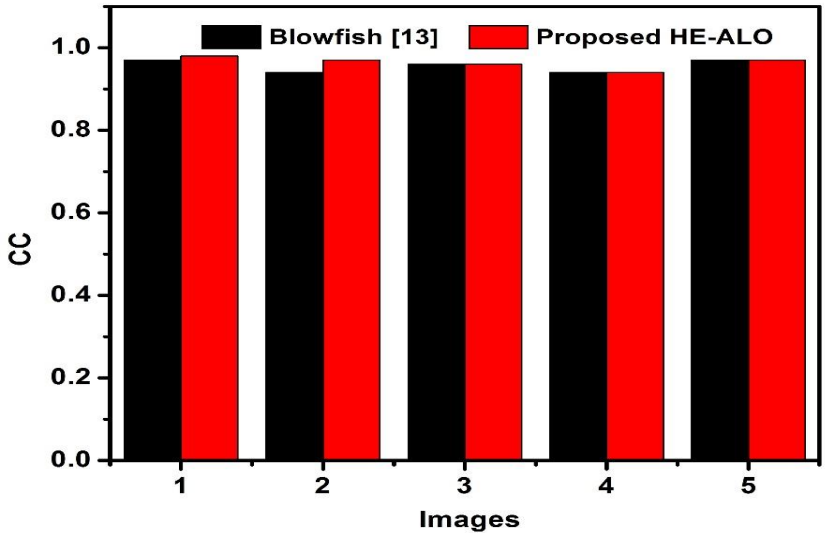


Figure 8. A comparison of the CC for the proposed HE-ALO with the Blowfish algorithm.

A comparison of different encryption and decryption modalities with existing approaches from literature is given in Figure 9. in terms of execution time for both the encryption and decryption phases.

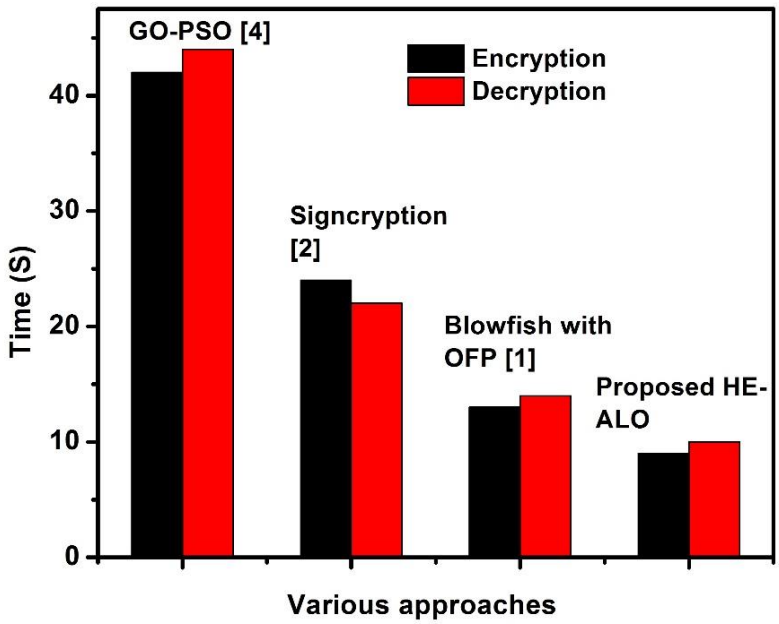


Figure 9. The execution time for both encryption and decryption phases of the proposed HE-ALO when compared with other approaches from literature.

Let us consider HE to encrypt the input medical images, as shown in Figure 10. The input medical image consists of multimodal images collected from the brain web and ADNI dataset. These datasets input images are arranged alphabetically.

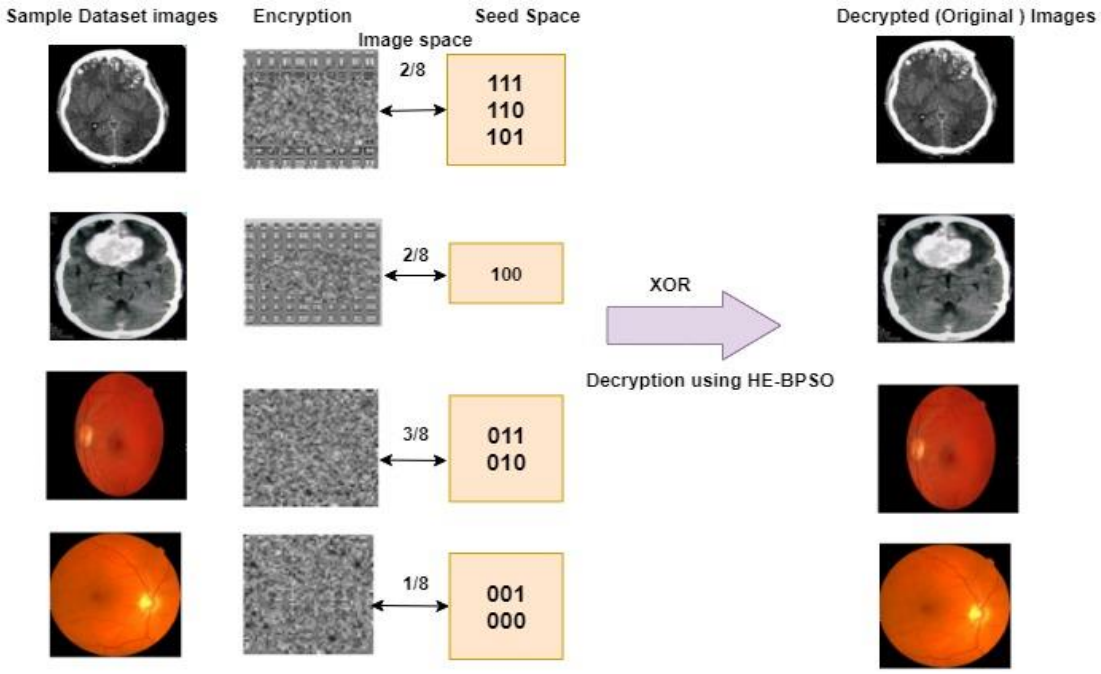
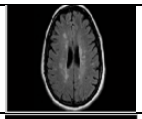
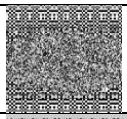
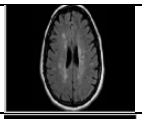
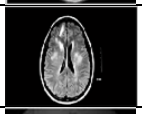
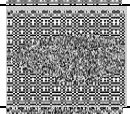
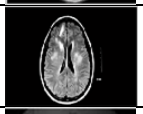
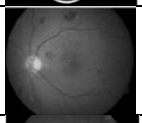
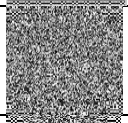
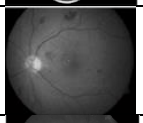
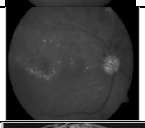
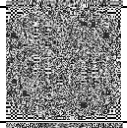
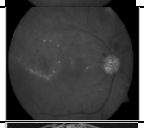
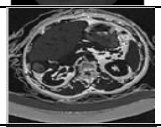
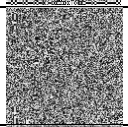
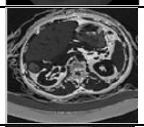
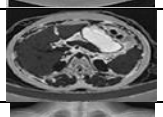
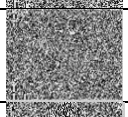
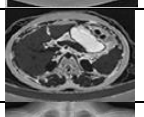
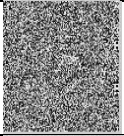
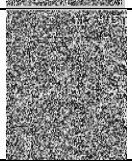


Figure 10. Graphical model for proposed HE-PSO

In Table 4, The proposed Honey Algorithm Encryption is optimized and compared with other existing algorithms like GO-PSO, Signcryption Algorithm, and Blowfish with OFP evaluation measures. At that point, the Medical imaging is encoded with the existing algorithms and the comparative analysis PSNR, MSE, BER and SSI also done and shown .HE algorithm that transmit the safe and reliable way of medical image .In order to get the picture back, decoding is achieved at the end. An efficient Image Encryption Comparative Result is shown .average estimation of HE algorithm is high than the other existing algorithms.This demonstrates that the HE algorithm also operates for an extensive range of medical images as well relationship coefficient is nearly unity. The MSE is determined by calculating the error in the medical image show in where the mean square error is low for the proposed method as it appears differently in comparison to the other comparable algorithm.

Table 4: An Efficient Image Encryption Comparative Result for HE-BPSO

Input	**Images**	**Encrypted Images**	**Decrypted Images**	**PSNR [6]**	**MSE [5]**	**BER [7]**	**SSI [8]**
Input1				62.69	0.10	0	1
Input2				63.93	0.07	0	1
Input3				61.21	0.08	0	1
Input4				62.89	0.09	0.01	1
Input5				64.79	0.08	0	0..9
Input6				61.91	0.08	0	0.9
Input7				59.31	0.10	0.01	1
Input8				60.39	0.07	0	0.9

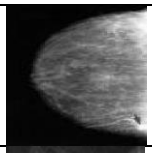
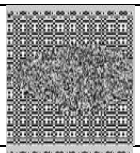
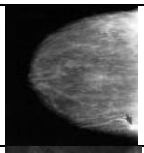
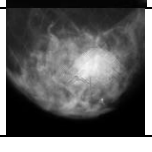
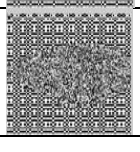
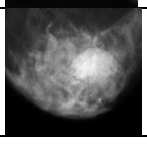
Input9				62.94	0.10	0	0.97
Input10				62.89	0.07	0.01	1

Figure 11 shows the comparative evaluation of PSNR for HE-BPSO technique compared with other conventional algorithms.

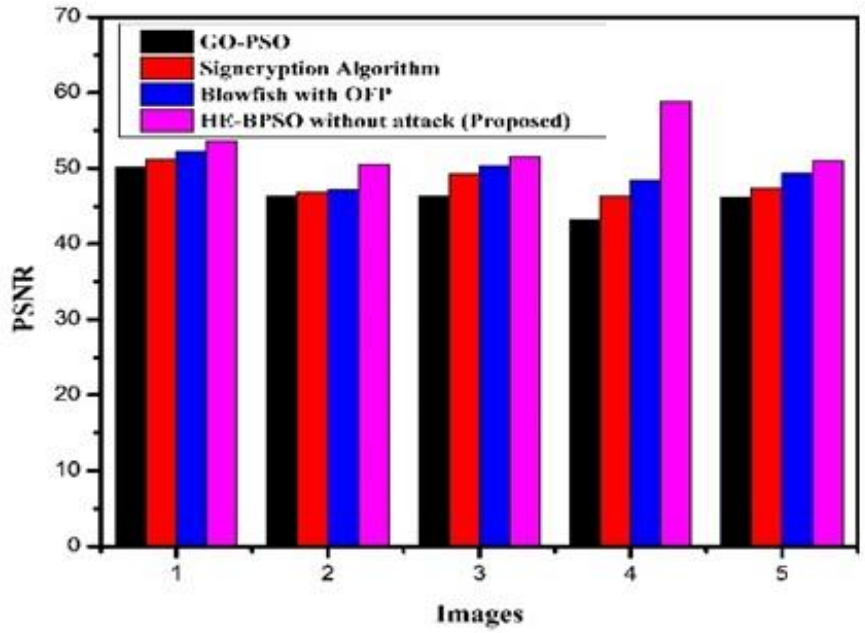


Figure 11. Comparative evaluation of PSNR for HE-BPSO with other conventional algorithms for 5 sample images.

Figure 12. shows the comparative evaluation results for BER parameter using Honey encryption and B-PSO.

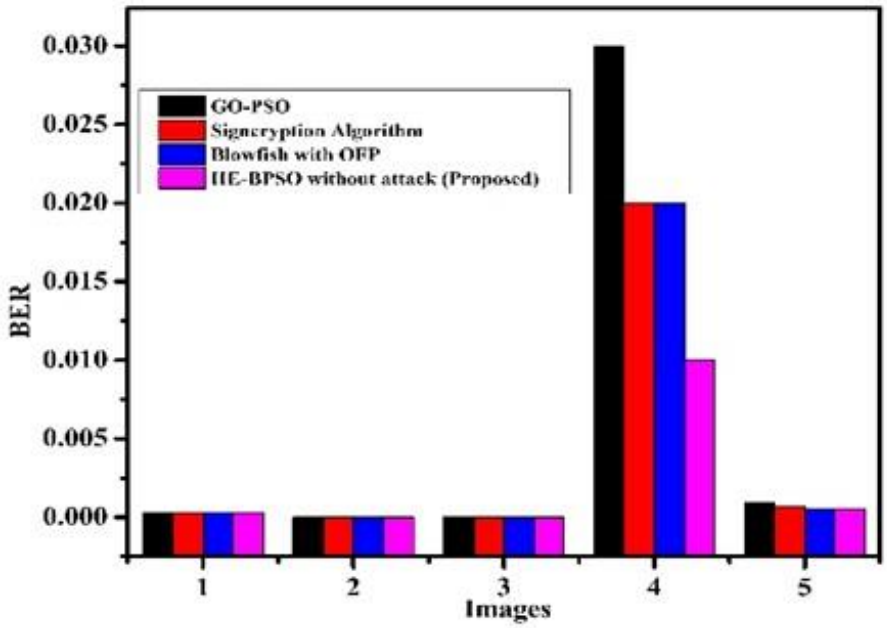


Figure 12. Comparative evaluation of BER for HE-BPSO with other conventional algorithms for 5 sample images.

The comparative evaluation of SSI parameter for the proposed HE-BPSO approach is done with other conventional algorithms for five samples, as shown in Figure 13.

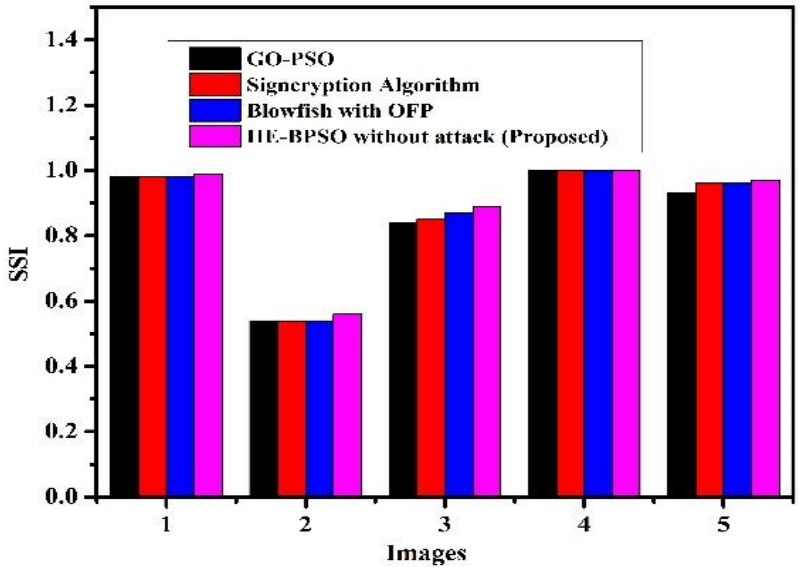


Figure 13. Comparative evaluation of SSI for HE-BPSO with other conventional algorithms for 5 sample images.

8. CONCLUSION

Medical imaging technology is one of the most critical applications that requires data protection. Encryption and decryption are used in this medical imaging system. The security key was created using a number of cryptographic methods to safeguard the data. Selecting a secure data transmission algorithm to achieve desirable qualities such as increased privacy, secrecy, integrity, and effectiveness. Honey encryption is utilised for secured imaging as well as Ant-Lion and later Binary PSO, which are employed for enhanced optimization of the brain web dataset image. The HE approach accurately calculated PSNR and MSE when compared to other current algorithms for particular parameters. When it comes to outcomes, honey beats the prior one out. Random keys are used for encryption and decryption by the Ant LION optimizer. The updated key is then improved by scrutinising every element and designing routes that engage the traps and latching devices. The mean square error (MSE) is reduced to 1% using this hybrid approach, while the peak signal-to-noise ratio (PSNR) is increased to 98% on average across all works. Compared to GOPSO, Signcryption, and Blowfish, which are all traditional algorithms, the PSNR figure is typically higher. The Honey Algorithm decreased processing time as well. Therefore, a honey algorithm with optimization techniques is used to study secure image encryption. These outcomes indicate that this system will be effective in the development of encryption and intrusion detection systems.

REFERENCES

1. T. Avudaiappan, R. Balasubramanian, S.S. Pandiyan, M. Saravanan, S.K. Lakshmanaprabu and K. Shankar, Medical image security using dual encryption with oppositional based optimization algorithm, *Journal of medical systems*, **42** (11) (2018), 1-11.
2. K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K. SatheshKumar, An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization, In Cybersecurity and Secure Information Systems, *Springer, Cham*, **15** (2) (2019), 31-42.
3. K. Shankar, M. Elhoseny, E.D. Chelvi, S.K. Lakshmanaprabu and W. Wu, An efficient optimal key based chaos function for medical image security, *IEEE Access*, **9** (6) (2018), 77145-77154.

4. M. Elhoseny, K. Shankar, S.K. Lakshmanaprabu, A. Maseleno and N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in Internet of Things, *Neural Computing and Applications*, **32** (15) (2020), 10979-10993.
5. S. Guhan, S. Arumugham, S. Janakiraman, A. Rengarajan and S. Rajagopalan, A Trio Approach Satisfying CIA Triad for Medical Image Security, *In International Conference on ISMAC in Computational Vision and Bio-Engineering, Springer, Cham*, **10** (2) (2018), 1109-1121.
6. K. Shankar and S.K. Lakshmanaprabu, Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm, *International Journal of Engineering & Technology*, **7** (9) (2018), 22-27.
7. A. Shehab, M. Elhoseny, K. Muhammad, A.K. Sangaiah, P. Yang, H. Huang and G. Hou, Secure and robust fragile watermarking scheme for medical images, *IEEE Access*, **6** (3) (2018), 10269-10278.
8. Z. Hua, S. Yi and Y. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Processing*, **144** (5) (2018), 134-144.
9. P. Praveenkumar, N.D. Kerthana, D. Ravichandran, J. Avila, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, Transreceiving of encrypted medical image–a cognitive approach, *Multimedia Tools and Applications*, **77** (7) (2018), 8393-8418.
10. A.A.A. El-Latif, B. Abd-El-Atty and M. Talha, Robust encryption of quantum medical images, *IEEE Access*, **6** (2) (2017), 1073-1081.
11. S. Thakur, A.K. Singh, S.P. Ghrera and A. Mohan, Chaotic based secure watermarking approach for medical images, *Multimedia Tools and Applications*, **79** (7) (2020), 4263-4276.
12. M. Gupta, K.K. Gupta and P.K. Shukla, Session key based fast, secure and lightweight image encryption algorithm, *Multimedia Tools and Applications*, **80** (7) (2021), 10391-10416.
13. M.J. Saddam, A.A. Ibrahim and A.H. Mohammed, A lightweight image encryption and blowfish decryption for the secure internet of things, In *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, *IEEE*, (2020), 1-5.
14. X. Zeng, A.T. Hammid, N.M. Kumar, U. Subramaniam and D.J. Almakhles, A grasshopper optimization algorithm for optimal short-term hydrothermal scheduling. *Energy Reports*, **7** (2) (2021), 314-323.

15. S. Mirjalili, S.M. Mirjalili and A. Hatamlou, Multi-verse optimizer: a nature-inspired algorithm for global optimization, *Neural Computing and Applications*, **27** (2) (2016), 495-513.
16. A.A. Abd El-Latif, B. Abd-El-Atty, M.S. Hossain, M.A. Rahman, A. Alamri and B.B. Gupta, Efficient quantum information hiding for remote medical image sharing, *IEEE Access*, **6** (3) (2018), 21075-21083.
17. S.M. Ismail, L.A. Said, A.G. Radwan, A. H. Madian and M.F. Abu-Elyazeed, Generalized double-humped logistic map-based medical image encryption, *Journal of Advanced Research*, **10** (1) (2018), 85-98.
18. L. Ma, L, Chen and S. Wang, Security analysis of a reversible watermarking algorithm for encrypted images in wavelet domain, *Multimedia Tools and Applications*, **78** (8) (2019), 9827-9843.

LIST OF PUBLICATIONS

1. G.J. Prabhu and B. Perumal, Medical Imaging Data Security using Effective Honey with Ant-Lion Optimization Algorithm, In *2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES), IEEE*, (2019), 1-5.
2. G.J. Prabhu and B. Perumal, A novel approach on medical imaging data security operation based on honey algorithm, In *Sustainable development in engineering and technology, 3ciencias*, (2022), 561-571.
3. G.J. Prabhu, B. Perumal, and T. Jarin, A Composite Medical Image Optimization Scheme Using Honey Encryption and Ant-Lion Algorithms for Secured Diagnostic Systems, *International Journal of Pattern Recognition and Artificial Intelligence*, (2022), DOI: 10.1142/S0218001422400043.
4. G.J. Prabhu, and B. Perumal, Multimodal Medical Imaging Security using Hybridization of Honey Encryption Algorithm with Binary Particle Swarm Optimization, *Turkish Journal of Computer and Mathematics Education*, **12** (10) (2021), 3905-3912.